(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-5909
(P2006-5909A)
(43)公開日　平成18年1月5日(2006.1.5)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
G09C 1/00	(2006.01)	G09C	1/00	660D	5K035
H04L 9/32	(2006.01)	H04L	9/00	675A	
H04L 29/14	(2006.01)	H04L	9/00	601E	
		H04L	13/00	315A	

審査請求 有　請求項の数 24　OL　（全 25 頁）

(21)出願番号　特願2005-126540 (P2005-126540)
(22)出願日　平成17年4月25日 (2005.4.25)
(31)優先権主張番号　特願2004-147795 (P2004-147795)
(32)優先日　平成16年5月18日 (2004.5.18)
(33)優先権主張国　日本国 (JP)

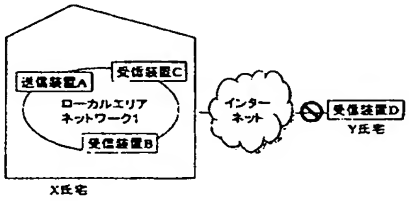
（特許庁注：以下のものは登録商標）
1．フロッピー

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100075812
弁理士　吉武　賢次
(74)代理人　100088889
弁理士　橋谷　英俊
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100096921
弁理士　吉元　弘
(74)代理人　100103263
弁理士　川崎　康

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法および情報処理プログラム

(57)【要約】
【課題】　コンテンツの不正利用を確実に防止し、かつコンテンツを有効利用する。
【解決手段】　本発明は、ネットワークを介して著作権保護のための暗号化されたコンテンツを伝送する送信装置と受信装置を備える。AKE/RTTフェーズにて用いるTCPコネクションとコンテンツ伝送フェーズに用いるTCPコネクションとが異なる。前者のTCPコネクションを用いて、送信装置と受信装置が個別に共有する値を用いて固有IDを暗号化して送信装置に送信し、送信装置は固有IDを固有IDテーブルに登録済みの固有IDであることを確認する。その確認が成功した場合には、送信装置は後者のTCPコネクションを用いて受信装置にコンテンツを暗号化して伝送する。
【選択図】　図1



【特許請求の範囲】
【請求項１】
ネットワークを介して通信装置に対して著作権保護のための暗号化されたコンテンツを送信する情報処理装置であって、
前記通信装置との間で第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、
前記第１の鍵を用いて生成された往復応答時間計測要求を前記第１の通信コネクションを用いて前記通信装置に送信して、該要求に対する計測要求応答が受信されるまでの往復応答時間を計測し、計測された往復応答時間が所定時間以内か否かをチェックし、かつ該計測要求応答の送信元が前記第１の鍵を共有する前記通信装置であることをチェックする往復応答時間計測手段と、
前記往復応答時間計測手段によるチェックが成功した場合に、前記第１の通信コネクションを用いて、前記第１の鍵で暗号化された前記通信装置に固有の識別情報を受信して、前記第１の鍵を用いて復号する固有ID受信手段と、
前記固有ID受信手段で復号された前記通信装置に固有の識別情報を登録するID登録手段と、
前記往復応答時間計測手段によるチェックが成功した場合に、前記第１の通信コネクションを用いて、コンテンツ送信に用いられる第２の鍵を前記第１の鍵で暗号化して前記通信装置に送信する共通鍵送信手段と、
第２の通信コネクションを用いて前記通信装置からのコンテンツ送信要求を受信し、このコンテンツ送信要求に含まれる前記第１の鍵で暗号化された前記通信装置に固有の識別情報を前記第１の鍵で復号するID復号手段と、
前記ID復号手段で復号された固有の識別情報が前記ID登録手段に登録されているか否かをチェックするIDチェック手段と、
前記通信装置に固有の識別情報が前記ID登録手段に登録されている場合には、前記通信装置から要求されたコンテンツを前記第２の鍵を用いて暗号化して、前記第２の通信コネクションを用いて前記通信装置に送信するコンテンツ送信手段と、を備えることを特徴とする情報処理装置。
【請求項２】
前記ID登録手段に前記固有の識別情報が登録されているならば、次回の往復応答時間計測を省略するRTT計測省略手段をさらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
コンテンツの送信中に前記ID登録手段から固有の識別情報を削除した場合に、前記第１の通信コネクションを用いて、前記通信装置に削除したことを通知する削除通知手段を備えることを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記通信装置との間で共有される往復応答時間計測要求識別情報と、第１の乱数と、前記通信装置から送信された第２の乱数と、前記第１の鍵とを用いて、第１の認証情報を生成する第１認証情報生成手段と、
前記通信装置から送信された計測要求応答に含まれる、計測要求応答識別情報と、前記第１および第２の乱数と、前記第１の鍵とを用いて前記通信装置が生成した第２の認証情報を受信して、その内容を前記第１の認証情報に基づいてチェックする認証情報チェック手段と、
前記認証情報チェック手段によるチェックに成功した場合に、前記通信装置に対して前記第１の認証情報のチェックを要求する認証情報チェック要求手段と、を備え、
前記往復応答時間計測手段は、UDPデータグラムのヘッダと、前記往復応答時間計測要求を行うたびに値が更新される前記往復応答時間計測要求識別情報に対応するシーケンス番号と、前記第１の乱数および前記シーケンス番号を含む往復応答時間計測要求とを送信し、UDPデータグラムのヘッダと、前記シーケンス番号と、前記第２の乱数および前記シ

ーケンス番号を含む計測要求応答とを受信することを特徴とする請求項１に記載の情報処理装置。

【請求項５】

前記IDチェック手段は、前記通信装置からのコンテンツ送信要求がHTTPでなされる場合には、HTTPリクエストヘッダに含まれる、前記第１の鍵で暗号化された前記通信装置に固有の識別情報を受信することを特徴とする請求項１に記載の情報処理装置。

【請求項６】

前記通信装置が送信した、往復応答時間計測要求の受信可能状態通知を受信する受信可能状態通知受信手段を備え、

前記往復応答時間計測手段は、前記受信可能状態通知を受信した後に、前記通信装置に往復応答時間計測要求を送信することを特徴とする請求項１に記載の情報処理装置。

【請求項７】

前記通信装置に往復応答時間計測要求を送信する前に、前記通信装置から送信された前記通信装置に固有の識別情報の検索要求を受信するID検索要求受信手段と、

この検索要求を受けて、前記通信装置に固有の識別情報が前記ID登録手段に登録されているか否かを検索するID検索手段と、

前記ID検索手段の検索結果を前記通信装置に送信する検索結果送信手段と、

前記通信装置から往復応答時間計測要求の不要通知を受信する不要通知手段と、を備え、

前記往復応答時間計測手段は、前記ID検索手段により前記ID登録手段への登録が確認され、かつ前記通信装置から往復応答時間計測要求の不要通知が受信された場合には、往復応答時間計測要求を中止することを特徴とする請求項１に記載の情報処理装置。

【請求項８】

ネットワークを介して通信装置に対して著作権保護のための暗号化されたコンテンツを送信する情報処理装置であって、

前記通信装置との間で第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、

前記第１の通信コネクションを用いて前記通信装置に往復応答時間計測要求を送信して、該要求に対する計測要求応答が受信されるまでの往復応答時間を計測し、計測された往復応答時間が所定時間以内か否かをチェックし、かつ該計測要求応答の送信元が前記第１の鍵を共有する前記通信装置であることをチェックする往復応答時間計測手段と、

前記往復応答時間計測手段によるチェックが成功した場合に、前記第１の通信コネクションを用いて、コンテンツ送信に用いられる第２の鍵を前記第１の鍵で暗号化して前記通信装置に送信する共通鍵送信手段と、

前記通信装置から要求されたコンテンツを前記第２の鍵を用いて暗号化して、第２の通信コネクションを用いて前記通信装置に送信するコンテンツ送信手段と、を備えることを特徴とする情報処理装置。

【請求項９】

前記往復応答時間計測手段によるチェック処理が成功した場合に、前記第１の通信コネクションを用いて、前記通信装置に固有の識別情報を登録するID登録手段を備えることを特徴とする請求項８に記載の情報処理装置。

【請求項１０】

前記ID登録手段に前記固有の識別情報が登録されているならば、次回の往復応答時間計測を省略するRTT計測省略手段をさらに備えることを特徴とする請求項９に記載の情報処理装置。

【請求項１１】

前記通信装置との間で共有される往復応答時間計測要求識別情報と、第１の乱数と、前記通信装置から送信された第２の乱数と、前記第１の鍵とを用いて、第１の認証情報を生成する第１認証情報生成手段と、

前記通信装置から送信された計測要求応答に含まれる、計測要求応答識別情報と、前記

第１および第２の乱数と、前記第１の鍵とを用いて前記通信装置が生成した第２の認証情報を受信して、その内容を前記第１の認証情報に基づいてチェックする認証情報チェック手段と、

前記認証情報チェック手段によるチェックに成功した場合に、前記通信装置に対して前記第１の認証情報のチェックを要求する認証情報チェック要求手段と、を備え、

前記往復応答時間計測手段は、前記往復応答時間計測要求を行うたびに値が更新される前記往復応答時間計測要求識別情報に対応するシーケンス番号と、前記シーケンス番号を含む往復応答時間計測要求とを送信し、前記シーケンス番号と、前記第２の乱数および前記シーケンス番号を含む計測要求応答とを受信することを特徴とする請求項８乃至１０のいずれかに記載の情報処理装置。

【請求項１２】

前記通信装置が送信した、往復応答時間計測要求の受信可能状態通知を受信する受信可能状態通知受信手段を備え、

前記往復応答時間計測手段は、前記受信可能状態通知を受信した後に、前記通信装置に往復応答時間計測要求を送信することを特徴とする請求項８乃至１１のいずれかに記載の情報処理装置。

【請求項１３】

前記通信装置に往復応答時間計測要求を送信する前に、前記通信装置から送信された前記通信装置に固有の識別情報の検索要求を受信するID検索要求受信手段と、

この検索要求を受けて、前記通信装置に固有の識別情報が前記ID登録手段に登録されているか否かを検索するID検索手段と、

前記ID検索手段の検索結果を前記通信装置に送信する検索結果送信手段と、

前記通信装置から往復応答時間計測要求の不要通知を受信する不要通知手段と、を備え、

前記往復応答時間計測手段は、前記ID検索手段により前記ID登録手段への登録が確認され、かつ前記通信装置から往復応答時間計測要求の不要通知が受信された場合には、往復応答時間計測要求を中止することを特徴とする請求項９に記載の情報処理装置。

【請求項１４】

ネットワークを介して通信装置から送信された、著作権保護のための暗号化されたコンテンツを受信する情報処理装置であって、

前記通信装置との間で第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、

前記通信装置からの往復応答時間計測要求を受信して、前記第１の鍵を用いて往復応答時間計測要求応答を送信する往復応答時間計測要求応答送信手段と、

前記通信装置との間で行われる往復応答時間計測が所定の条件を満たす場合に、前記第１の通信コネクションを用いて、固有の識別情報を前記第１の鍵で暗号化して前記通信装置に送信するID送信手段と、

往復応答時間計測が所定の条件を満たす場合に前記通信装置が前記第１の通信コネクションを用いて送信した、前記第１の鍵で暗号化された第２の鍵を受信する共通鍵受信手段と、

第２の通信コネクションを用いてコンテンツ要求を前記通信装置に送信するコンテンツ要求送信手段と、

前記通信装置が前記第２の通信コネクションを用いて送信した、前記第２の鍵を用いて暗号化されたコンテンツを受信して、前記第２の鍵で復号するコンテンツ受信手段と、を備えることを特徴とする情報処理装置。

【請求項１５】

前記通信装置との間で共有される往復応答時間計測要求応答識別情報と、第１の乱数と、前記通信装置から送信された第２の乱数と、前記第１の鍵とを用いて生成された第１の認証情報を生成する第１認証情報生成手段と、

前記通信装置から送信された往復応答時間計測要求に含まれる、往復応答時間計測要求

識別情報と、前記第１および第２の乱数と、前記第１の鍵とを用いて生成された第２の認証情報を受信して、その内容を前記第１の認証情報に基づいてチェックする認証情報チェック手段と、

前記認証情報チェック手段によるチェック結果を前記通信装置に送信するチェック結果送信手段と、を備え、

前記往復応答時間計測要求応答送信手段は、UDPデータグラムのヘッダと、往復応答時間計測要求を行うたびに更新される前記往復応答時間計測要応答に対応するシーケンス番号と、前記第２の乱数および前記シーケンス番号を含む往復応答時間計測要求を受信し、UDPデータグラムのヘッダと、前記シーケンス番号と、前記第１の乱数および前記シーケンス番号を含む往復応答時間計測要求応答を送信することを特徴とする請求項１４に記載の情報処理装置。

【請求項１６】

前記ID送信手段は、コンテンツ送信要求をHTTPで行う場合には、固有の識別情報を前記第１の鍵で暗号化してHTTPリクエストヘッダに含めて前記通信装置に送信することを特徴とする請求項１４に記載の情報処理装置。

【請求項１７】

前記通信装置からの往復応答時間計測要求を受信可能であることを示す受信可能状態通知を送信する受信可能状態通知送信手段を備えることを特徴とする請求項１４に記載の情報処理装置。

【請求項１８】

前記通信装置からの往復応答時間計測要求を受信する前に、固有の識別情報を前記通信装置が保持するか否かを検索するよう要求するID検索要求送信手段と、

この検索要求を受けて前記通信装置が検索した結果を受信する検索結果受信手段と、

前記検索結果受信手段で受信された結果に基づいて、前記通信装置が固有の識別情報を保持することが検知された場合には、前記通信装置に対して往復応答時間計測要求が不要である旨を通知する計測要求不要通知手段と、を備えることを特徴とする請求項１４に記載の情報処理装置。

【請求項１９】

ネットワークを介して通信装置から送信された、著作権保護のための暗号化されたコンテンツを受信する情報処理装置であって、

前記通信装置との間で、第１の通信コネクションを用いて、認証要求と、固有の識別情報を前記通信装置に送信するＩＤ送信手段と、

前記通信装置との間で前記第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、

前記通信装置からの往復応答時間計測要求を受信して、前記第１の鍵を用いて往復応答時間計測要求応答を送信する往復応答時間計測要求応答送信手段と、

往復応答時間計測が所定の条件を満たす場合に前記通信装置が前記第１の通信コネクションを用いて送信した、前記第１の鍵で暗号化された第２の鍵を受信する共通鍵受信手段と、

第２の通信コネクションを用いてコンテンツ要求を前記通信装置に送信するコンテンツ要求送信手段と、

前記通信装置が前記第２の通信コネクションを用いて送信した、前記第２の鍵を用いて暗号化されたコンテンツを受信して、前記第２の鍵を用いて復号するコンテンツ受信手段と、を備えることを特徴とする情報処理装置。

【請求項２０】

前記通信装置との間で共有される往復応答時間計測要求応答識別情報と、第１の乱数と、前記通信装置から送信された第２の乱数と、前記第１の鍵とを用いて生成された第１の認証情報を生成する第１認証情報生成手段と、

前記通信装置から送信された往復応答時間計測要求に含まれる、往復応答時間計測要求識別情報と、前記第１および第２の乱数と、前記第１の鍵とを用いて生成された第２の認

証情報を受信して、その内容を前記第１の認証情報に基づいてチェックする認証情報チェック手段と、

前記認証情報チェック手段によるチェック結果を前記通信装置に送信するチェック結果送信手段と、を備え、

前記往復応答時間計測要求応答送信手段は、往復応答時間計測要求を行うたびに更新される前記往復応答時間計測要求に対応するシーケンス番号と、前記第２の乱数および前記シーケンス番号を含む往復応答時間計測要求を受信し、前記シーケンス番号と、前記第１の乱数および前記シーケンス番号を含む往復応答時間計測要求応答を送信することを特徴とする請求項１９に記載の情報処理装置。

【請求項２１】

前記通信装置からの往復応答時間計測要求を受信可能であることを示す受信可能状態通知を送信する受信可能状態通知送信手段を備えることを特徴とする請求項１９に記載の情報処理装置。

【請求項２２】

前記通信装置からの往復応答時間計測要求を受信する前に、固有の識別情報を前記通信装置が保持するか否かを検索するよう要求するID検索要求送信手段と、

この検索要求を受けて前記通信装置が検索した結果を受信する検索結果受信手段と、

前記検索結果受信手段で受信された結果に基づいて、前記通信装置が固有の識別情報を保持することが検知された場合には、前記通信装置に対して往復応答時間計測要求が不要である旨を通知する計測要求不要通知手段と、を備えることを特徴とする請求項１９に記載の情報処理装置。

【請求項２３】

ネットワークを介して第１の通信装置から第２の通信装置に対して著作権保護のための暗号化されたコンテンツを送信する情報処理方法であって、

前記第１および第２の通信装置は、互いに第１の通信コネクションを用いて認証・鍵交換処理を行い、前記第１および第２の通信装置との間でのみ共有する第１の鍵を生成し、

前記第１の通信装置は、前記第１の通信コネクションを用いて前記第２の通信装置に往復応答時間計測要求を送信して、該要求に対する計測要求応答が受信されるまでの往復応答時間を計測し、計測された往復応答時間が所定時間以内かをチェックし、かつ前記第１の通信装置が前記第１の鍵を共有するか否かをチェックし、

前記第１の通信装置は、両チェックが成功した場合に、前記第１の通信コネクションを用いて、コンテンツ送信に用いられる第２の鍵を前記第１の鍵で暗号化して前記第２の通信装置に送信し、

前記第１の通信装置は、前記第２の通信装置から要求されたコンテンツを前記第２の鍵を用いて暗号化して、第２の通信コネクションを用いて前記第２の通信装置に送信することを特徴とする情報処理方法。

【請求項２４】

ネットワークを介して第１の通信装置から第２の通信装置に対して著作権保護のための暗号化されたコンテンツを送信する、コンピュータにより実行可能な情報処理プログラムであって、

前記第１および第２の通信装置の間で、第１の通信コネクションを用いて認証・鍵交換処理を行い、前記第１および第２の通信装置との間でのみ共有する第１の鍵を生成するステップと、

前記第１の通信コネクションを用いて前記第１の通信装置から前記第２の通信装置に往復応答時間計測要求を送信して、該要求に対する計測要求応答が受信されるまでの往復応答時間を前記第１の通信装置にて計測し、計測された往復応答時間が所定時間以内かを前記第１の通信装置にてチェックし、かつ前記第１の通信装置が前記第１の鍵を共有するか否かをチェックするステップと、

両チェックが成功した場合に、前記第１の通信コネクションを用いて、コンテンツ送信に用いられる第２の鍵を前記第１の鍵で暗号化して前記第１の通信装置から前記第２の通

信装置に送信するステップと、
前記第２の通信装置から要求されたコンテンツを前記第２の鍵を用いて暗号化して、第２の通信コネクションを用いて前記第１の通信装置から前記第２の通信装置に送信するステップとを備えることを特徴とする情報処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、著作権保護の必要な各種コンテンツを送信または受信する情報処理装置、情報プログラムおよび情報処理方法に関する。
【背景技術】
【０００２】
ブロードバンドや無線LAN等のコンピュータネットワークの普及や、デジタル技術の進展に伴い、通信機能を備えたデジタル情報機器（以下、デジタル家電）と呼ばれる製品が普及しつつある。また、地上波デジタル放送の開始に伴い、デジタル放送対応のテレビやセットトップボックス、DVDレコーダ等が、今後より一層普及することが予想される。複数のデジタル家電がネットワークに接続されれば、利用者はネットワーク経由でコンテンツを楽しむことができ、有益である（特許文献１参照）。
【０００３】
ここで、コンテンツとは、各種のデジタルデータ、たとえばMPEG2やMPEG4などの動画データや音声データ、テキストデータや画像データのようなドキュメント・データなどを指す。この種のデジタルデータからなるコンテンツは劣化することなく容易に複製することが可能であるという利点を持つ反面、コンテンツの著作権に関して注意を払わなければならない。たとえば、著作権を保護すべきコンテンツを、ある送信装置から受信装置に送信する場合を考える。著作権を保護すべきコンテンツをやり取りする範囲は、一定の範囲内、たとえば著作権30条の私的利用の範囲内などの正当な権限の範囲内か、それよりもさらに狭い範囲内に制限され、その範囲を超えて第三者とのでコンテンツをやり取りできないように制限するのが望ましい。
【特許文献１】特開2003-194491公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、AVデータの伝送をIP(インターネットプロトコル)で行う場合、IPはケーブル長などの物理的な制約なくデータを伝送できるため、著作権法上の問題が生じるおそれがある。たとえば、IPではVPN(Virtual Private Network)といった、遠隔のIPネットワーク同士を論理的に接続する汎用的な技術がある。この技術を用いると、A地区のX氏宅のホームネットワーク内に接続された装置と、(A地区とは物理的に離れた)B地区のY氏宅のホームネットワーク内に論理的に接続し、データの伝送が可能となる。つまり、X氏宅のコンテンツがX氏宅内のホームネットワークに閉じず、遠隔地のY氏もX氏のホームネットワークに接続してX氏の所有するコンテンツを閲覧することができてしまう。
【０００５】
本発明は、上記の問題点に鑑みてなされたものであり、その目的は、コンテンツの不正利用を確実に防止し、かつコンテンツを有効利用可能な情報処理装置、情報処理方法および情報処理プログラムを提供することにある。
【課題を解決するための手段】
【０００６】
本発明の一態様によれば、ネットワークを介して通信装置に対して著作権保護のための暗号化されたコンテンツを送信する情報処理装置であって、前記通信装置との間で第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、前記第１の鍵を用いて生成された往復応答時間計測要求を前記第１の通信コネクションを用いて前記通信装置に送信して、該要求に対す

る計測要求応答が受信されるまでの往復応答時間を計測し、計測された往復応答時間が所定時間以内か否かをチェックし、かつ該計測要求応答の送信元が前記第１の鍵を共有する前記通信装置であることをチェックする往復応答時間計測手段と、前記往復応答時間計測手段によるチェックが成功した場合に、前記第１の通信コネクションを用いて、前記第１の鍵で暗号化された前記通信装置に固有の識別情報を受信して、前記第１の鍵を用いて復号する固有ID受信手段と、前記固有ID受信手段で復号された前記通信装置に固有の識別情報を登録するID登録手段と、前記往復応答時間計測手段によるチェックが成功した場合に、前記第１の通信コネクションを用いて、コンテンツ送信に用いられる第２の鍵を前記第１の鍵で暗号化して前記通信装置に送信する共通鍵送信手段と、第２の通信コネクションを用いて前記通信装置からのコンテンツ送信要求を受信し、このコンテンツ送信要求に含まれる前記第１の鍵で暗号化された前記通信装置に固有の識別情報を前記第１の鍵で復号するID復号手段と、前記ID復号手段で復号された固有の識別情報が前記ID登録手段に登録されているか否かをチェックするIDチェック手段と、前記通信装置に固有の識別情報が前記ID登録手段に登録されている場合には、前記通信装置から要求されたコンテンツを前記第２の鍵を用いて暗号化して、前記第２の通信コネクションを用いて前記通信装置に送信するコンテンツ送信手段と、を備えることを特徴とする情報処理装置が提供される。

【０００７】

本発明の一態様によれば、ネットワークを介して通信装置に対して著作権保護のための暗号化されたコンテンツを送信する情報処理装置であって、前記通信装置との間で第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、前記第１の通信コネクションを用いて前記通信装置に往復応答時間計測要求を送信して、該要求に対する計測要求応答が受信されるまでの往復応答時間を計測し、計測された往復応答時間が所定時間以内か否かをチェックし、かつ該計測要求応答の送信元が前記第１の鍵を共有する前記通信装置であることをチェックする往復応答時間計測手段と、前記往復応答時間計測手段によるチェックが成功した場合に、前記第１の通信コネクションを用いて、コンテンツ送信に用いられる第２の鍵を前記第１の鍵で暗号化して前記通信装置に送信する共通鍵送信手段と、前記通信装置から要求されたコンテンツを前記第２の鍵を用いて暗号化して、第２の通信コネクションを用いて前記通信装置に送信するコンテンツ送信手段と、を備えることを特徴とする情報処理装置が提供される。

【０００８】

また、本発明の一態様によれば、ネットワークを介して通信装置から送信された、著作権保護のための暗号化されたコンテンツを受信する情報処理装置であって、前記通信装置との間で第１の通信コネクションを用いて認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、前記通信装置からの往復応答時間計測要求を受信して、前記第１の鍵を用いて往復応答時間計測要求応答を送信する往復応答時間計測要求応答送信手段と、前記通信装置との間で行われる往復応答時間計測が所定の条件を満たす場合に、前記第１の通信コネクションを用いて、固有の識別情報を前記第１の鍵で暗号化して前記通信装置に送信するID送信手段と、往復応答時間計測が所定の条件を満たす場合に前記通信装置が前記第１の通信コネクションを用いて送信した、前記第１の鍵で暗号化された第２の鍵を受信する共通鍵受信手段と、第２の通信コネクションを用いてコンテンツ要求を前記通信装置に送信するコンテンツ要求送信手段と、前記通信装置が前記第２の通信コネクションを用いて送信した、前記第２の鍵を用いて暗号化されたコンテンツを受信して、前記第２の鍵で復号するコンテンツ受信手段と、を備えることを特徴とする情報処理装置が提供される。

【０００９】

また、本発明の一態様によれば、ネットワークを介して通信装置から送信された、著作権保護のための暗号化されたコンテンツを受信する情報処理装置であって、前記通信装置との間で、第１の通信コネクションを用いて、認証要求と、固有の識別情報を前記通信装置に送信するＩＤ送信手段と、前記通信装置との間で前記第１の通信コネクションを用い

て認証・鍵交換処理を行い、前記通信装置との間でのみ共有する第１の鍵を生成する認証・鍵交換手段と、前記通信装置からの往復応答時間計測要求を受信して、前記第１の鍵を用いて往復応答時間計測要求応答を送信する往復応答時間計測要求応答送信手段と、往復応答時間計測が所定の条件を満たす場合に前記通信装置が前記第１の通信コネクションを用いて送信した、前記第１の鍵で暗号化された第２の鍵を受信する共通鍵受信手段と、第２の通信コネクションを用いてコンテンツ要求を前記通信装置に送信するコンテンツ要求送信手段と、前記通信装置が前記第２の通信コネクションを用いて送信した、前記第２の鍵を用いて暗号化されたコンテンツを受信して、前記第２の鍵で復号するコンテンツ受信手段と、を備えることを特徴とする情報処理装置が提供される。

【発明の効果】

【００１０】

本発明によれば、宅内などの距離的に限定された範囲内でのみ、コンテンツの送受信を許可するため、コンテンツの不正利用を確実に防止できるとともに、コンテンツの有効利用を図ることができる。

【発明を実施するための最良の形態】

【００１１】

以下、図面を参照しながら、本発明の一実施形態について説明する。

【００１２】

（第１の実施形態）

図１は本発明に係る情報処理装置を備えたコンテンツ送受信システムの概略構成を示すブロック図である。図１のコンテンツ送受信システムは、個人の楽しむ範囲内で主にAVデータを送受信することを目的としており、ローカルエリアネットワーク１に接続された送信装置Ａ、受信装置Ｂ、受信装置C、インターネットを経由してローカルエリアネットワーク１に接続された受信装置Dを備えている。なお、インターネットに接続された受信装置Dと、ローカルエリアネットワークとは不図示のルータ装置等で接続されていてもよい。送信装置Ａと受信装置Ｂ～Ｄの少なくとも一つが本発明の情報処理装置の一態様である。

【００１３】

ローカルエリアネットワーク１の物理レイヤおよびリンクレイヤは、IEEE802.11に準拠した無線LAN、イーサネット(登録商標)、IEEE1394などの種々の形態を採りうる。ローカルエリアネットワーク１のネットワークレイヤは、インターネットプロトコル(以下、単にIPと呼ぶ)が使用されている場合には、IPv4でもよいし、IPv6でもよい。また、ローカルエリアネットワーク１には送信装置Ａ、受信装置Ｂ、受信装置C以外の装置が接続されていてもよいが、簡略化のためここでは省略している。

【００１４】

ここで、コンテンツとは例えばMPEG2,MPEG4のような動画データや、MP3のような音声データ、またはテキストデータや画像データのようなドキュメントなどデジタルコンテンツを指す。ここでは説明を簡単にするため、著作権保護をかけた上で伝送すべきデジタルコンテンツ（以下、単にコンテンツと呼ぶ）である場合を考える。

【００１５】

さて、送信装置Ａから受信装置Ｂ、C、Dにコンテンツを送信する場合を考える。この時、注意すべきはコンテンツの著作権である。前述したように、当該コンテンツをやり取りする範囲は、一定の範囲内、例えば、著作権法第30条に記載の私的使用の範囲内などの正当な権限の範囲内あるいはそれよりもさらに狭い範囲内に制限され、その範囲を超えて、たとえば他人間でのコンテンツのやりとりはできないようにすることが望ましい。すなわち、X氏の所有する送信装置Ａから受信装置Ｂ、受信装置Cへはコンテンツの送受信を許可するが、所有者の異なる受信装置Dへはコンテンツを送信しないようにすることを実現する。

【００１６】

本実施形態は、大きく分けて３つの特徴を有する。

【００１７】
（第１の特徴）
伝送経路がIPの場合、物理的な距離の制約を受けることなくデータを送受信することができる。このため、コンテンツが家庭内IPネットワークの範囲を超えて送信装置から受信装置に伝送されてしまう。
【００１８】
そこで、本実施形態では、送信装置と受信装置がある一定の距離内に存在することを確認するために往復応答時間(Round Trip Time:以下、単にRTTを呼ぶ)を用いる。すなわち、送信装置と受信装置の間でコンテンツの伝送に先立ち、RTTを計測し、計測値がある一定の閾値以下である場合にはコンテンツの送信を許可する。RTTが閾値を超えた場合にはコンテンツの送信を拒否する。
【００１９】
（第２の特徴）
家庭内ネットワークの構成によっては、送信装置と受信装置の間にルータやブリッジ装置が介在することがある。例えば、有線インターフェースを備えた送信装置と、無線インターフェースを備えた受信装置が通信する場合には、メディア間をブリッジするために無線アクセスポイントを用いることが一般的である。
【００２０】
ここで、仮に送信装置と受信装置以外の他の装置間で無線アクセスポイントを経由した大量のトラヒックが発生したとすると、トラヒックがない状態に比べて無線アクセスポイントがブリッジ処理に要する時間は相対的に大きくなり、結果として送信装置と受信装置の間で測定されるRTTが大きくなってしまう。
【００２１】
この問題を回避するためにRTTの閾値を必要以上に大きく設定してしまうと、今度は家庭内ネットワークに接続した送信装置と、家庭外に設置した受信装置との間で通信が可能となってしまい、第１の特徴が実現できなくなる。このように、RTTをIP以上のレイヤで規定する場合、伝送経路上のトラヒック量による影響を受けやすいため、閾値の決定が非常に難しい。
【００２２】
そこで、コンテンツの送受信時に送信装置と受信装置が毎回RTTの測定を行うのではなく、一旦送信装置と受信装置の間でRTT計測が成功した場合には、一方の装置に備わった固有IDを他方の装置に登録し、登録された装置であればRTTの計測を省略できるものとする。これにより、家庭内ネットワークにトラヒックがない状態でRTTの計測に成功して固有IDの登録処理が完了していれば、次回接続時にはトラヒックの状態に関係なく登録した装置間でコンテンツの送受信が可能となる。またRTTの閾値は、トラヒックがない状態に限定して定めることが可能となる。
【００２３】
（第３の特徴）
固有IDの登録確認処理にてコンテンツの送受信を許可してしまうと、送信装置と受信装置を固有IDの登録処理時にのみ近い位置に持ってくれば、コンテンツ送受信時には物理的な距離に関係なく通信可能となってしまう。すなわち、送信装置と受信装置を近距離に設置し、RTT計測を行って固有IDを登録すれば、その後は、受信装置を宅外に持ち出して利用できることになる。
【００２４】
そこで、送信装置から受信装置へのコンテンツの出力時間やデータ量を計測し、所定時間（所定量）のコンテンツを送信すると、登録した固有IDを消去する。これにより、第１および第２の特徴を実現でき、かつ利便性を損なうことなく、第３の特徴も実現できる。
【００２５】
上述した第１～第３の特徴を実現するために、本実施形態では、コンテンツの配布範囲を限定する手法として、送信装置と受信装置の間で、コンテンツの伝送に先立ち、予め往

復応答時間を計測して、互いの装置が近距離にあることを確認した上で、互いの装置、あるいは一方の装置の固有IDを他方の装置に「登録」する手順を設ける。またコンテンツの送受信時に登録処理が完了しているか否かの確認処理を行い、かつ固有IDの登録有効期間を設ける、という仕組みを導入する。

【００２６】

以下では、図１の受信装置Ｂが送信装置Ａに対してコンテンツの送信要求を行って、コンテンツの提供を受ける例について説明する。

【００２７】

図２は本発明に係る送信装置Ａの一実施形態の概略構成を示すブロック図である。図２に示すように、送信装置Ａはネットワークインターフェース部１１と、パケット処理部１２と、データコネクション管理部１３と、認証・鍵交換コネクション管理部１４と、認証・鍵交換処理部１５と、RTT計測部１６と、固有ID管理部１７と、送信データ管理部１８と、暗号処理部１９と、コンテンツ供給部２０を有する。

【００２８】

ネットワークインターフェース部１１は、受信装置Ｂと通信を行うための物理レイヤ処理およびデータリンクレイヤ処理を実行する。パケット処理部１２は、受信装置Ｂと通信を行うためのネットワークレイヤ・トランスポートレイヤ処理を実行する。認証・鍵交換処理部１５は、受信装置Ｂと認証・鍵交換処理を行う。データコネクション管理部１３はコンテンツ送受信用のコネクションを管理する。認証・鍵交換コネクション管理部１４は認証・鍵交換用のコネクションを管理する。

【００２９】

認証・鍵交換処理部１５は、認証・鍵交換処理が成功すると、各受信装置との間でコンテンツを暗号化したり復号化したりするのに用いる秘密鍵として、個別共有鍵"Ｋｐ"と共通共有鍵"Ｋｓ"を利用する。個別共有鍵"Ｋｐ"とは、認証・鍵交換処理の途中で相互に送信しあう乱数を用いて送信装置と受信装置がそれぞれ計算し、個別に生成する鍵のことを指す。共通共有鍵"Ｋｓ"とは、認証・鍵交換処理が成功したすべての受信装置との間で共有する鍵のことを指す。Ｋｓはコンテンツの暗号化・復号化に用いる。Ｋｐは送信装置がＫｓを受信装置に送信する際の鍵としたり、受信装置が自機器の固有IDを暗号化して送信装置に送信したりする際の鍵として用いる。図３に送信装置と受信装置がそれぞれ個別共有鍵"Ｋｐ"と共通共有鍵"Ｋｓ"を共有する様子を図示する。

【００３０】

ここで、認証・鍵交換処理とは、送信装置や受信装置があるライセンス機関から正しくライセンスをうけた装置であることを相互に認証し、正当な装置であると確認できた場合に、共通の鍵を生成する処理のことを指す。認証の方法として、ISO/IEC 9798-3やISO/IEC 9798-2のような公知の手法を用いればよい。

【００３１】

暗号処理部１９は、認証・鍵交換処理によって共有した鍵を用いてコンテンツ、乱数および固有IDを暗号化する。これらのデータを暗号・復号化するための暗号アルゴリズムとしては、AESなどの公知の手法を用いればよい。コンテンツ供給部２０は、コンテンツを暗号処理部１９に供給する。

【００３２】

RTT計測部１６は、受信装置Ｂとの間でRTTの計測を行い、得られた値が閾値以下か否かを判別し、その結果を認証・鍵交換処理部に伝える。固有ID管理部１７は、内部に固有IDリスト２１を有する。

【００３３】

図４は固有ID管理部１７に格納されている固有IDリスト２１の一例を示す図である。固有IDリスト２１は、必須項目とオプション項目で構成される。必須項目として、他の通信装置(受信装置Ｂ)の固有IDを有し、オプション項目として固有IDリスト２１に登録された登録日時や、ネットワークインターフェース部11のMACアドレスなど通信装置に固有の情報を有する。

【００３４】
なお、固有IDリスト２１は、有限個数(たとえばN個)の固有IDを記録することができるものとする。すなわち固有ID管理部１７は固有IDリスト２１を格納するためのRAM領域を持つ。
【００３５】
RTT計測部１６が受信装置との間で行うRTT計測処理において、計測結果として得られたRTTがある一定の閾値以下であると判断された場合に限り、通信相手から固有IDを受信し、固有IDリスト２１に当該通信装置の固有IDを追加する。
【００３６】
送信装置Ａや受信装置Ｂに備わっている固有IDは、製造業者に拠らず、ライセンスに従って一意のIDを持つことが望ましい。仮に固有IDが既に固有IDリスト２１に存在する場合は、その旨を認証・鍵交換処理部に通知する。
【００３７】
なお、固有IDリスト２１のオプション項目として登録日時を有する場合は、固有ID登録時にこの日時を更新してもよい。また、すでにN個の固有IDが記録されている場合には、新たな固有IDの追加を拒否するか、あるいはオプション項目として登録日時がある場合は最も古い登録日時の固有IDを削除した後、当該固有IDを追加するか、あるいはユーザにどの固有IDを削除するか選択を促すメッセージを表示し、任意の固有IDを削除してもよい。また、固有ID管理部１７は、受信装置から受信した固有IDが当該IDリストに記載されているかの検索処理を実行する。
【００３８】
送信データ管理部１８は、受信装置に送信したコンテンツの送信時間または送信したデータ量を、受信装置ごとに計測して記録する。送信相手の受信装置を区別するには、固有IDリストに登録された固有IDを用いればよい。暗号処理部１９は、送信装置Ａが送信するコンテンツを暗号化する。
【００３９】
以下の例では、パケット処理部にて処理された情報を、インターネットプロトコルにて伝送することを想定する。
【００４０】
図５は本発明に係わる受信装置Ｂの一実施形態の概略構成を示すブロック図である。図５に示すように、受信装置Ｂはネットワークインターフェース部３１と、パケット処理部３２と、データコネクション管理部３３と、認証・鍵交換コネクション管理部３４と、認証・鍵交換処理部３５と、RTT応答部３６と、固有ID管理部３７と、暗号処理部３８と、コンテンツ処理部３９とを有する。
【００４１】
ネットワークインターフェース部３１は、送信装置Ａと通信を行うための物理レイヤ処理およびデータリンクレイヤ処理を実行する。パケット処理部３２は、送信装置Ａと通信を行うためのネットワークレイヤ・トランスポートレイヤ処理を実行する。認証・鍵交換処理部３５は、送信装置Ａと認証・鍵交換処理を行う。データコネクション管理部３３は、コンテンツ送受信用のコネクションを管理する。認証・鍵交換コネクション管理部３４は、認証・鍵交換用のコネクションを管理する。RTT応答部３６は、送信装置Ａから送信されたRTT要求に基づきRTTに関する応答処理を行う。固有ID管理部３７は、受信装置Ｂの固有IDを格納し、送信装置Ａに固有IDを送信する。暗号処理部３８は、受信したコンテンツを復号したり固有IDを暗号化したりする。コンテンツ処理部３９は、受信したコンテンツを表示装置などに出力したり蓄積したりするための処理を行う。
【００４２】
なお、ネットワークインターフェース部３１、パケット処理部３２および認証・鍵交換処理部３５については、送信装置Ａと同様のものを用いればよい。
【００４３】
（処理シーケンス：AKE/RTT計測フェーズ）

図６は送信装置Ａと受信装置Ｂとの間で行われる全体的な処理手順の一例を示すシーケンス図である。本実施形態は、送信装置Ａから受信装置Ｂにコンテンツを伝送するに際して、「AKE/RTT計測フェーズ」と「コンテンツ伝送フェーズ」の2つの処理を行う。

【００４４】

「AKE/RTT計測フェーズ」とは、送信装置Ａと受信装置Ｂが認証・鍵交換処理とRTT計測処理を行うフェーズである。

【００４５】

「コンテンツ伝送フェーズ」とは、コンテンツの伝送に先立ち、送信装置Ａが受信装置Ｂの固有IDを保有しているか否かを検査するID登録確認処理とコンテンツの伝送処理を行うフェーズである。

【００４６】

「AKE/RTT計測フェーズ」は必ず「コンテンツ伝送フェーズ」に先立ち行われる。AKE/RTT計測フェーズにおける認証・鍵交換のためのTCPコネクションは、コンテンツ伝送フェーズにおけるコンテンツ伝送のためのTCPコネクションとは異なっている。すなわち、認証・鍵交換のためのTCPポートとコンテンツ伝送フェーズのためのTCPポートには、互いに異なる番号が割り振られている。

【００４７】

まず、送信装置は、受信装置との間で認証・鍵交換処理を行う（ステップＳ１）。これにより、送信装置と受信装置は個別共有鍵Ｋpを生成して共有する（ステップＳ２，Ｓ３）。次に、送信装置と受信装置はRTTの計測を行う（ステップＳ４）。

【００４８】

RTTが一定の閾値以内であれば、受信装置は送信装置に対して固有のIDを送信し（ステップＳ５）、これを受信した送信装置は該固有IDを固有IDリスト２１に登録する。最後に、送信装置は共通共有鍵Ｋsを生成し（ステップＳ６）、Ｋpで暗号化した後、受信装置に送信する（ステップＳ７，Ｓ８）。これにより、受信装置と送信装置は共通共有鍵Ｋsを共有することになる。以上がAKE/RTTフェーズで行われる処理の概要である。

【００４９】

その後、コンテンツ伝送フェーズが行われる。まず受信装置はコンテンツ送信要求を送信装置に送信する（ステップＳ９）。次に、受信装置は自身の固有IDを送信装置に送信し（ステップＳ１０）、送信装置はこの固有IDが固有IDリスト２１に登録されているか検索処理を行う（ステップＳ１１）。この確認処理により、送信装置に受信装置の固有IDが登録されていることが確認されると、コンテンツをAKE/RTT伝送フェーズにて生成した共通共有鍵Ｋsにて暗号化して送信する。

【００５０】

以下、「AKE/RTT計測フェーズ」と「コンテンツ伝送フェーズ」について詳しく述べる。

【００５１】

（AKE/RTT計測フェーズの第１例）

図７は送信装置Ａと受信装置Ｂの間でなされるAKE/RTT計測フェーズの処理手順の一例を示すシーケンス図である。図７に示すAKE/RTT計測処理では、送信装置Ａと受信装置ＢのRTTを測定し、受信装置Ｂの固有IDを送信装置Ａに登録する。

【００５２】

まず、送信装置Ａと受信装置Ｂは、互いに正当な装置であるか否かの認証処理と鍵交換処理を行い（ステップＳ２１）、個別共有鍵Ｋpを共有する（ステップＳ２２，Ｓ２３）。認証が失敗した場合には、所定のエラー処理を行い、以後の処理は行われない。

【００５３】

また、送信装置と受信装置が互いに以下のRTT計測処理を行う能力があるかを、認証・鍵交換処理の途中で交換しあう証明書のバージョン番号にて判別してもよい。証明書に記述されたバージョン番号がある特定のバージョン以上の場合には、認証・鍵交換処理に引き続いてRTT計測処理を行い、そうでない場合にはRTT計測処理を行わずに送信装置は共通

共有鍵Ｋｓを生成し、Ｋｐで暗号化した後、受信装置に送信する。

【００５４】

次に、受信装置と送信装置はそれぞれ初期値、乱数および個別共有鍵Ｋｐを用いてメッセージ認証コード(MAC:Message Authentication Code、以下単にMACと呼ぶ)を生成する（ステップＳ２４，Ｓ２５）。MACは以下の（１）および（２）式に示すように、個別共有鍵Ｋｐにて、初期値N、乱数Ra、Rbを暗号化した値のうち、上位Xビットと下位Yビットを用いればよい。MAC-1a，MAC-2aは送信装置で生成され、MAC-1b，MAC-2bは受信装置で生成される。送信装置がMAC-1aを受信装置に送信して、受信装置でMAC-1bと比較する。また、受信装置がMAC-2bを送信装置に送信して、送信装置でMAC-2aと比較する。

MAC-1a = MAC1b = Encryption(Ｋｐ，Ra || Rb || N)上位Xbit　…（１）

MAC-2a = MAC2b = Encryption(Ｋｐ，Ra || Rb || N)下位Ybit　…（２）

【００５５】

ここで、乱数Ra,Rbは認証・鍵交換処理にて用いた値を再利用してもよいし、MACの生成に先立ち、送信装置と受信装置がそれぞれRa、Rbを生成して平文にて互いに交換してもよい。また、Nは送信装置と受信装置があらかじめ共有して持つ初期値である。Nは特に秘密とする値ではないため、ここでの共有とは単に仕様書等で記載された値という意味にすぎず、MACの生成に先立ち、送信装置から受信装置に平文にて送信することでNの値を通知してもよい。以後Nをシーケンス番号と呼ぶ。

【００５６】

乱数Ra、Rb、初期値Nを暗号化するための暗号アルゴリズムには、AESなどの公知の手法を用いればよい。仮にMAC-1とMAC-2のビット長が暗号ブロックよりも長い値を必要とするならば、CBCモードなどの公知の技術を用いて暗号ブロックをチェーンさせればよい。

【００５７】

上述した（１）式および（２）式では、個別共有鍵Ｋｐを用いてMACを生成しているが、個別共有鍵Ｋｐの代わりに共通共有鍵Ｋｓを用いてMACを生成してもよい。

【００５８】

次に、受信装置はMACの計算処理が成功したことを通知するRTT受信可能状態通知を送信装置に送信する（ステップＳ２６）。RTT受信可能状態通知を送信する理由は、受信装置は、送信装置のRTT要求に対して即座にRTT応答を返信する必要があるためである。仮にMAC計算処理を実行中にRTT要求を受信した場合、何も計算負荷がない状態に比べて、返信までに要する時間が大きくなると考えられる。従って、受信装置はMAC計算処理を予め行っておくことが望ましい。このため、RTT要求に対して即座に応答できる準備が整ったことを送信装置に通知するために、RTT受信可能状態通知を送信する。

【００５９】

この状態通知を受信した送信装置は、シーケンス番号Nにて、先に計算したMAC-1aをRTT要求に挿入して送信する（ステップＳ２７）。この時、RTTの時間計測を開始する（ステップＳ２８）。

【００６０】

RTT要求を受信した受信装置は、その応答として、受信したシーケンス番号Nに対応するMAC-2aをRTT応答に挿入して送信装置に返信する（ステップＳ２９）。

【００６１】

図８はRTT要求とこれに続くRTT応答のパケットフォーマットの一例を示す図である。図８に示すように、RTTはUDPデータグラムとして伝送される。RTTに用いるUDPデータグラムのペイロードは必須項目とオプション項目に分けられる。必須項目には、命令タイプ、シーケンス番号、データの3項目があり、オプション項目にはバージョン番号がある。命令タイプは、RTT要求かRTT応答かを区別するフィールドである。シーケンス番号は送信装置から受信装置に送られた複数のRTT要求とRTT応答を区別するためのフィールドであり、MACの計算に用いた値Nがここに入る。送信装置はRTT要求のためのUDPデータグラムを送信するたびにこのNの値を一定の値ずつ(たとえば1ずつ）増加させる。RTT要求の場合、データ部にはシーケンス番号Nにて計算した（１）式に示すMAC-1aが、RTT応答の場合データ部に

はシーケンス番号Nにて計算した（２）式に示すMAC-2bが入る。

【００６２】

送信装置は、RTT応答を受信すると、時間計測を終了して、RTT要求を送信してから経過した時間を測定する（ステップＳ３０）。仮にこの測定結果があらかじめ定められた閾値以下であれば、RTT応答にて受信したMAC-2aと送信装置内で計算したMAC-2bが一致するかチェック処理を行う（ステップＳ３１）。

【００６３】

仮にチェック処理が成功すれば、一致したMACのシーケンス番号(N)を通知するメッセージ(MACチェック要求)を受信装置に送信する（ステップＳ３２）。

【００６４】

このメッセージを受信した受信装置はRTT要求のデータ部に入っているMAC-1aと、あらかじめ計算しておいたMAC-1bが一致するかチェックする（ステップＳ３３）。このMAC-1bは送信装置から受信したN(ステップ３２)を用いて計算し、さらにMAC-1aは送信装置から受信したシーケンス番号Nのペイロードに記載された値を用いる。仮に一致していれば、一致したことを伝えるメッセージと受信装置の固有IDを暗号化して送信する(MACチェック応答)（ステップＳ３４）。この時、暗号化の鍵として個別共有鍵Ｋpを用いる。送信装置は固有IDを復号化し、固有ID管理部の固有IDリスト２１に登録する（ステップＳ３５）。

【００６５】

最後に送信装置は共通共有鍵Ｋsを生成し（ステップＳ３６）、Ｋpで暗号化した後、受信装置に送信する（ステップＳ３７，Ｓ３８）。なお、図７に示すシーケンスでは、共通共有鍵Ksの送信（ステップS３７、S３８）を独立したコマンドとして定義しているが、送信装置側でRTT計測の閾値チェックとMACの検証処理が成功した時点でKsを送信すればよく、MACチェック要求（ステップS３２）でシーケンス番号NとKpで暗号化したKsを同時に送信するようにしてもよい。

【００６６】

なお、このID登録処理については、MACチェック応答にて送信する固有IDを用いるほかに、認証・鍵交換処理の際で送信装置と受信装置が交換する証明書の中に含まれる固有IDを用いる方法もある。

【００６７】

上述したRTT要求とRTT応答にはUDPを用いるが、受信装置がどのポート番号でRTT要求を受信可能であるのか、RTT要求のあて先ポート番号を送信装置に事前に知らせておく必要がある。この手法として、（１）送信装置と受信装置があらかじめ仕様書等で定められた値を共有しておく手法、（２）RTT受信可能状態通知にて送信装置に通知する手法、（３）受信装置が送信装置にUDPポート番号を通知するコマンドを定義し、RTT要求に先立ち送信装置に当該コマンドで通知する手法、（４）認証・鍵交換に用いるTCPコネクションと同じUDPのポート番号を利用する方法、などがある。

【００６８】

（AKE/RTT計測フェーズの第２例）

AKE/RTT計測フェーズの第２例は、すでに受信装置の固有IDが送信装置の固有IDリスト２１に登録されており、受信装置と送信装置がRTTチェック処理を行わずに、認証・鍵交換処理のみを行う点に特徴がある。上述した第２の特徴で述べたように、いったん送信装置と受信装置との間でRTTチェック処理が成功して送信装置の固有IDリスト２１に受信装置の固有IDが登録されたならば、次回以降はRTTチェック処理を行わず、受信装置の固有IDが登録されているかどうかのID登録確認処理のみを行えばよい。

【００６９】

図９はRTTチェック処理を行わずID登録確認処理のみを行う場合の処理手順の一例を示すシーケンス図である。認証・鍵交換処理を行い、送信装置と受信装置が個別共有鍵を生成するまでの処理（ステップＳ４１～Ｓ４５）は、図７のステップＳ２１～Ｓ２５と同様である。

【００７０】

その後、図７の処理では、受信装置がRTT受信可能状態通知を送信したが、本実施形態では、その代わりに、受信装置Ｂが送信装置Ａに受信装置Bの固有IDを含めたID検索要求を送信する（ステップＳ４６）。なお、ID検索要求に含める固有IDは暗号化してもよいし、しなくてもよい。

【００７１】

ID検索要求を受信した送信装置は、自身の固有IDリスト２１に通信中の受信装置の固有IDが含まれるか検索処理を行い（ステップＳ４７）、ID検索要求の応答にその結果を返す（ステップＳ４８）。

【００７２】

この例では、認証・鍵交換処理以前に送信装置と受信装置との間でRTTチェック処理が行われていることが前提となっているため、ID検索結果としてIDが含まれていることを示すメッセージが返信されている。なお、固有IDとして認証・鍵交換に用いる証明書に記載の固有IDを用いる場合には、認証・鍵交換処理にて送信装置に対し、受信装置の固有IDを送信することになるため、送信装置は通信対象の受信装置の固有IDを固有IDリストに有しているか否かを認証・鍵交換処理の途中で判別することができるが、このID検索要求に受信装置の固有IDを含めてもよい。なお、その場合には固有IDは暗号化せずに平文で送信すればよい。

【００７３】

受信装置は、自身の固有IDが送信装置の固有IDリスト２１に含まれていることを知ると、RTT不要通知を送信装置に送信する（ステップＳ４９）。RTT不要通知を受信した送信装置は、共通共有鍵Ｋsを生成して（ステップＳ５０）、個別共有鍵Ｋpにて暗号化して受信装置に送信する（ステップＳ５１，Ｓ５２）。

【００７４】

なお、受信装置が送信装置の固有IDリスト２１に自身の固有IDが含まれていることを別の手段によりあらかじめ知っているならば、ID検索要求とそれに続くID検索結果をスキップして、RTT不要通知を送信してもよい。

【００７５】

また、受信装置がRTT不要通知を送信装置に送信する際、受信装置の固有IDをRTT不要通知に含めて送信し、さらに送信装置が固有IDリスト２１に当該固有IDが含まれているか検索処理を行うようにしてもよい。

【００７６】

（コンテンツ伝送フェーズ）

次に、コンテンツ伝送フェーズについて述べる。図１０は送信装置Ａと受信装置Ｂの間で行われるコンテンツ伝送フェーズの処理手順の一例を示すシーケンス図である。まず、受信装置は、自身が所有する共通共有鍵Ｋsを送信装置が保持しているか確認するために、Ｋs番号の確認要求を送信する（ステップＳ６１）。送信装置は自身の所有するＫsに対応したＫs番号を送信する（ステップＳ６２）。受信装置は、送信装置から送信されたＫs番号が、自身が所持するＫs番号と一致するか否かをチェックする（ステップＳ６３）。

【００７７】

AKE/RTT計測フェーズとコンテンツ伝送フェーズは、必ずしも連続して行われるとは限らず、時間的に離れて実行される場合がある。この間に送信装置が再起動処理などを行い、Ｋsを更新してしまうと、受信装置はこれを検出する手段がない。従って、受信装置は、これからコンテンツを要求する相手である送信装置が自身と同じＫsを共有しているかを確認するために、上述したＫs確認処理を行う。もちろん、AKE/RTT計測フェーズに引き続き、すぐさまコンテンツ伝送フェーズに移行する場合など、明らかに送信装置と受信装置が同一のＫsを共有していると受信装置が判断できる場合には、このＫs確認処理は省略してもよい。

【００７８】

次に、受信装置はコンテンツ送信要求を送信する（ステップＳ６４）。このコンテンツ送信要求には、自身の固有IDを個別共有鍵Ｋpにて暗号化した値を含める。コンテンツのA

V伝送プロトコルにHTTPを用いる場合、コンテンツ送信要求はHTTP GETリクエストに相当するが、このGETリクエストのリクエストヘッダの1エンティティとして暗号化した固有IDを含めればよい。

【００７９】

コンテンツ送信要求を受信した送信装置は、暗号化された受信装置の固有IDを個別共有鍵Ｋpを用いて復号し、自装置の固有IDリスト２１に当該固有IDが含まれているか検索処理を実行する（ステップＳ６５）。仮に含まれている場合には、通信相手である受信装置がRTTチェック済みのであることを意味しているため、コンテンツを共有共通鍵Ｋsで暗号化して送信する（ステップＳ６６）。なお、コンテンツ送信時に送信されるHTTP Responseヘッダに、ID登録確認処理が成功したことを示すメッセージをエンティティとして含めてもよい。

【００８０】

ここで、重要なことは、受信装置が自身の固有IDを送信する際に、送信装置と受信装置の間でのみ共有する鍵Ｋpを用いて暗号化する点である。単に固有IDを伝送する際、送信装置と受信装置以外の他の装置に推測できないようにして送信するだけであれば、たとえば送信装置が認証・鍵交換処理が成功した各受信装置との間で共有する値Ｋsを用いればよい。

【００８１】

図９の処理シーケンスでは、RTTチェック処理を行わず、ID登録確認処理のみを行う手順について示したが、上述した第３の特徴で述べたように、送信装置が固有IDリスト２１に受信装置の固有IDを登録しておく期間には制限が設けられる。すなわち、送信装置はコンテンツの送信時間や送信量を計測し、所定時間または所定量だけコンテンツを送信した場合に登録した固有IDを消去する。このように、固有IDの登録期間を計測するために、送信装置はコンテンツ送信に先立ち、どの受信装置からのコンテンツ送信要求であるかを管理する必要がある。

【００８２】

図１１は共通共有鍵Ｋsを用いて受信装置の固有IDを暗号化した場合に問題となる処理手順の一例を示すシーケンス図である。図１１では受信装置ＡおよびＢが送信装置と共通共有鍵Ｋsを共有しているものとする。

【００８３】

まず、受信装置Ａは自身の固有IDをＫsで暗号化してコンテンツ送信要求を送信する（ステップＳ８１）。ここで悪意のある装置Ｘがこの暗号化した固有IDをコピーして機器内に保存したとする（ステップＳ８２）。

【００８４】

次に、受信装置Ｂは自身の固有IDを同一のＫsで暗号化して送信する（ステップＳ８３）。このとき装置Ｘは先に取得した固有ID Aとすりかえて送信装置に伝送する（ステップＳ８４）。すると送信装置は受信装置Ｂからのコンテンツ送信要求であるにもかかわらず、受信装置Ａからの要求であると判断し、受信装置Ａの送信データ量の計測を始めてしまう（ステップＳ８５）。コンテンツは共通共有鍵Ｋsで暗号化して送信されるため（ステップＳ８６）、Ｋsをもつ受信装置Ｂはこれを復号することができてしまう。

【００８５】

このように、本実施形態では、AKE/RTTフェーズにて用いるTCPコネクションとコンテンツ伝送フェーズに用いるTCPコネクションとが異なる。前者のTCPコネクションを用いて、送信装置と受信装置が個別に共有する値を用いて固有IDを暗号化して送信装置に送信し、送信装置は受信した固有IDが固有IDテーブルに登録済みであることを確認する。その確認が成功した場合には、送信装置は後者のTCPコネクションを用いて受信装置にコンテンツを暗号化して伝送する。

【００８６】

図９では受信装置の固有IDが送信装置の固有IDリスト２１に登録されているか否かを調査する方法について示したが、これらID検索要求とID検索結果を定義する手法として、こ

のほかにも（１）HTTPヘッダに含める手法、（２）認証・鍵交換のコマンドの一つとして定義する手法がある。

【００８７】

HTTPヘッダに含める手法では、ID検索要求をHTTP Requestヘッダの1エンティティとして定義し、自身の固有IDを個別共有鍵Ｋpで暗号化してHTTP HEADリクエストの中に挿入し、送信装置に送信する。HEADリクエストとは、受信装置がコンテンツそのものではなく、コンテンツのバイト長などの付属情報を取得するために定義されたHTTPのコマンドの一つである。このHTTP HEADリクエストを受信した送信装置は、受信装置の固有IDが固有IDリスト２１に含まれていれば、そのことを示すResponseコードを返し、そうでなければHTTPのエラーメッセージコードを返す。この処理はHTTPのリクエストを送信するという意味において、図１０に示したコンテンツ送受信用TCPコネクションと同様の処理であり、コンテンツ伝送処理部とID検索処理部とを共用させることができ、機器の構成を簡略化することができる。

【００８８】

上述したように、本実施形態によれば、RTTによってコンテンツの伝送範囲を制限することができる。RTTは伝送経路の物理レイヤや伝送経路上のトラヒックによって変化するため、送信装置と受信装置が家庭内ネットワークに接続されていたとしても、必ずしも一回でRTTチェックが成功するとは限らない。このような理由から、RTT要求とRTT応答は連続して何回もなされることを考慮して、RTT要求とRTT応答のパケットにシーケンス番号をつけて、何度目のRTT計測かを識別できるようにする。

【００８９】

また、RTT要求とRTT応答が正しい通信相手から送信されたことを確認するために、送信装置と受信装置が認証・鍵交換処理によって共有する個別共有鍵を用いてMACを生成し、これを検証する。

【００９０】

さらに、受信装置は送信装置から受信したRTT要求に対して即座にRTT応答を返す必要があるが、受信装置の処理能力によっては、RTT要求を受信してからMACを計算していたのでは、短時間でRTT応答を返すことができない。従って、事前にMACを計算できるようにし、かつそのMACが正しい値であったか否かを後から検証できるようにする。

【００９１】

また、本実施形態では、AKE/RTT計測フェーズに用いるTCPコネクションを、コンテンツ伝送フェーズに用いるTCPコネクションとは別にしている。AKE/RTT計測フェーズとコンテンツ伝送フェーズは、時間的に離れて行われることがあるが、仮に複数の受信装置がネットワーク上に存在する場合、送信装置側からみると、どの受信装置からのコンテンツ送信要求であるか、またその受信装置がAKE/RTTフェーズを行ったことがあり、ID登録が完了しているか否かを判別する必要がある。このため、本実施形態の受信装置は、コンテンツ送信要求に加えて、個別共有鍵Ｋpにて自身の固有IDを暗号化して送信することにより、確かにID登録が完了した装置であることを送信装置に伝達できる。

【００９２】

（エラー処理）

次に、エラー処理について説明する。図１２～図１６までは送信装置または受信装置でエラーが生じた場合の処理動作の一例を示すシーケンス図である。

【００９３】

（エラー処理：送信装置側のエラーによる失敗例）

図１２はRTTチェック処理にて受信装置から受信したRTT応答が一定の閾値を超えた場合のエラー処理の一例を示すシーケンス図である。受信装置からRTT応答を受信するまでの処理（ステップＳ９１～Ｓ９７）は図７に示したものと同様の手順でよい。

【００９４】

送信装置がRTTの閾値のチェックに失敗すると（ステップＳ９８）、受信装置に対してRTTチェック処理が失敗したことを通知するメッセージを送信して（ステップＳ９９）、シ

ーケンス番号Nを更新して新たなメッセージ認証コードMAC-1c,MAC-2cを計算する（ステップＳ１０１）。また、RTT失敗通知を受信した送信装置は、シーケンス番号Nを更新して新たなメッセージ認証コードMAC-1d,2dを計算する（ステップＳ１００，Ｓ１０２）。MAC-1c,MAC-1d,MAC-2c,MAC-2dは以下の（３）および（４）式で計算される。

MAC-1c = MAC1d = Encryption(Kp, Ra || Rb || N+1)上位Xbit　…（３）

MAC-2c = MAC2d = Encryption(Kp, Ra || Rb || N+1)下位Ybit　…（４）

【００９５】

ここで、シーケンス番号は1ずつ更新される例を示している。この再計算したMACを使って、RTTチェック処理を繰り返す（ステップＳ１０３～Ｓ１１０）。

【００９６】

図１２に示した例では、RTT計測処理が失敗した後、MACの再計算処理を行っている。送信装置ないし受信装置の計算能力が低く、MACの計算処理に時間がかかる場合には、RTTチェック処理が成功するまでに要する所要時間が長くなってしまう。これを改善する処理手順が図１３に示されている。

【００９７】

図１３では、送信装置と受信装置がRTTチェック処理に先立ち、あらかじめ複数のメッセージ認証コードを計算して、自装置に保存しておく（ステップＳ１２１～Ｓ１２４）。受信装置はMACの計算が終了するとRTT受信可能状態通知を送信装置に送信する（ステップＳ１２５）。この通知を受けた送信装置は、かりにRTTチェック処理が失敗したとしても（ステップＳ１２６～Ｓ１３０）、RTT失敗通知を送信することなく、順にRTT要求を送信する（ステップＳ１３１～Ｓ１３５）。これによりMACの再計算とRTT失敗通知・応答に要する時間を省略することができ、短時間により多くのRTTチェック処理を行うことができる。

【００９８】

なお、RTT要求とRTT応答はUDPにより送受信されるため、通信系路上でパケットが消失してしまうと、再送信されない。このため、送信装置は必ずしもRTT応答を受信できるとは限らない。そこで、送信装置はRTT要求を送信してから一定時間以内にRTT応答を受信しない場合には、次のRTT要求を送信するように、タイムアウトの閾値を定めてもよい。また、このタイムアウト処理によるRTT要求の回数を計測し、タイムアウトが継続して発生するならば、RTTチェック処理を中止するような機能を設けてもよい。

【００９９】

また、RTT要求が繰り返し送信される場合、最終的にRTTチェック処理が成功するまで時間がかかり、認証・鍵交換処理用のTCPコネクションがタイムアウト処理により切断してしまう可能性がある。これを防ぐために、RTTチェック処理中は一定時間内にNULLデータを送信するなどして認証・鍵交換処理用のTCPコネクションが切断されないようにしてもよい。

【０１００】

図１４はコンテンツ伝送フェーズにて送信装置側でID登録確認処理が失敗した場合のエラー処理の一例を示すシーケンス図である。第３の特徴で述べたように、送信装置は受信装置に対して一定量のデータを送信すると、当該受信装置の固有IDを破棄する（ステップＳ１４７）。したがって、受信装置は、次の認証・鍵交換処理時にRTTチェック処理を再度行う必要がある（ステップＳ１４９）。

【０１０１】

このように送信装置に固有IDが登録されていない状態でコンテンツ送信要求を受信した場合には、送信装置はコンテンツの送信を拒否する。この拒否メッセージとしては、（１）HTTP GETリクエストに応答するResponseの1エンティティに、ID確認処理が失敗したことを示すメッセージを定義する手法、（２）コンテンツが存在しないといったRFC2616に定義されたHTTP Responseのエラーコードを送信する手法、（３）認証・鍵交換処理に用いるコマンドの一つとして定義する手法、などがある。

【０１０２】

なお、図１５に示すように、送信装置が受信装置の固有IDを破棄する際（ステップＳ１６７）、そのことを受信装置に通知するコマンドを定義してもよい（ステップＳ１７０）。その場合、受信装置は次回コンテンツ要求に先立ち、RTTチェック処理を行い、再度自身の固有IDを送信装置に登録する必要がある。

【０１０３】

（エラー処理：受信装置側のエラーによる失敗例）

次に、受信装置側でのエラーが発生した場合の処理手順について説明する。

【０１０４】

図１６は、MACチェック処理においてMAC-1a,MAC-1bの検査に失敗した場合に、送信装置にエラーメッセージを送信する場合の処理手順の一例を示すシーケンス図である。送信装置と受信装置で認証・鍵交換処理を行い（ステップＳ１８１）、認証・鍵交換に成功すると、送信装置と受信装置がそれぞれ個別共有鍵Ｋpを生成する（ステップＳ１８２，Ｓ１８３）。

【０１０５】

その後、図１３と同様の手順で、RTT要求とRTT応答を行い（ステップＳ１８４～Ｓ１８９）。送信装置がRTTのチェックとメッセージ認証コードMAC 2a/2bの一致検査に成功すると（ステップＳ１９０）、送信装置は受信装置に対してMACチェック要求を行う（ステップＳ１９１）。

【０１０６】

受信装置がメッセージ認証コードMAC 2a/2bの一致検査に失敗すると（ステップＳ１９２）、受信装置は送信装置に対して、失敗した旨のMACチェック応答を行う（ステップＳ１９３）。

【０１０７】

その後、送信装置と受信装置はそれぞれエラー処理を行う（ステップＳ１９４，Ｓ１９５）。

【０１０８】

図１７は受信装置が行うエラー処理の一例を示すシーケンス図である。送信装置が受信装置の固有IDを固有IDリスト２１に登録した後（ステップＳ２０４）、送信装置の電源がオフしたり、通信ケーブルが抜けたりしたとする。この場合、自動的に、固有IDリスト２１に登録された固有IDは破棄される。

【０１０９】

その後、受信装置が送信装置に対して、共通共有鍵Ｋs番号の確認要求を行うと（ステップＳ２０５）、送信装置は受信装置に対して、自己が所持する共通共有鍵Ｋs番号を送信する（ステップＳ２０６）。これを受信した受信装置は、共通共有鍵Ｋs番号の一致検査を行い（ステップＳ２０７）、この場合は失敗する。したがって、受信装置は、所定のエラー処理を行う（ステップＳ２０８）。

【０１１０】

上述した実施形態で説明した送信装置および受信装置の少なくとも一部は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、送信装置や受信装置の少なくとも一部の機能を実現するプログラムをフロッピーディスクやＣＤ－ＲＯＭ等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【０１１１】

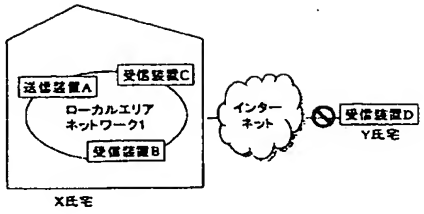
また、送信装置や受信装置の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【図面の簡単な説明】

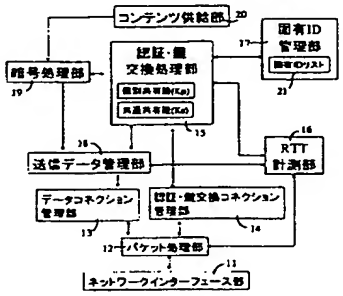
【０１１２】

【図１】本発明に係る情報処理装置を備えたコンテンツ送受信システムの概略構成を示すブロック図。
【図２】本発明に係る送信装置Ａの一実施形態の概略構成を示すブロック図。
【図３】送信装置と受信装置との間の認証・鍵交換を説明する図。
【図４】固有ID管理部１７に格納されている固有IDリスト２１の一例を示す図。
【図５】本発明に係わる受信装置Ｂの一実施形態の概略構成を示すブロック図。
【図６】送信装置Ａと受信装置Ｂとの間で行われる全体的な処理手順の一例を示すシーケンス図。
【図７】送信装置Ａと受信装置Ｂの間でなされるAKE/RTT計測フェーズの処理手順の一例を示すシーケンス図。
【図８】RTT要求とこれに続くRTT応答のパケットフォーマットの一例を示す図。
【図９】RTTチェック処理を行わずID登録確認処理のみを行う場合の処理手順の一例を示すシーケンス図。
【図１０】送信装置Ａと受信装置Ｂの間で行われるコンテンツ伝送フェーズの処理手順の一例を示すシーケンス図。
【図１１】共通共有鍵Ｋsを用いて受信装置の固有IDを暗号化した場合に問題となる処理手順の一例を示すシーケンス図。
【図１２】RTTチェック処理にて受信装置から受信したRTT応答が一定の閾値を超えた場合のエラー処理の一例を示すシーケンス図。
【図１３】図１２の処理を改善する処理の一例を示すシーケンス図。
【図１４】コンテンツ伝送フェーズにて送信装置側でID登録確認処理が失敗した場合のエラー処理の一例を示すシーケンス図。
【図１５】送信装置が受信装置の固有IDを破棄する際に、そのことを受信装置に通知するコマンドを定義する処理の一例を示すシーケンス図。
【図１６】MACチェック処理においてMAC-1a,MAC-1bの検査に失敗した場合に、送信装置にエラーメッセージを送信する場合の処理手順の一例を示すシーケンス図。
【図１７】受信装置が行うエラー処理の一例を示すシーケンス図。
【符号の説明】
【０１１３】
１１　ネットワークインターフェース部
１２　パケット処理部
１３　データコネクション処理部
１４　認証・鍵交換コネクション処理部
１５　認証・鍵交換処理部
１６　RTT計測部
１７　固有ID管理部
１８　送信データ管理部
１９　暗号処理部
２０　コンテンツ供給部
３１　ネットワークインターフェース部
３２　パケット処理部
３３　データコネクション処理部
３４　認証・鍵交換コネクション管理部
３５　認証・鍵交換処理部
３６　RTT応答部
３７　固有ID管理部
３８　暗号処理部
３９　コンテンツ処理部

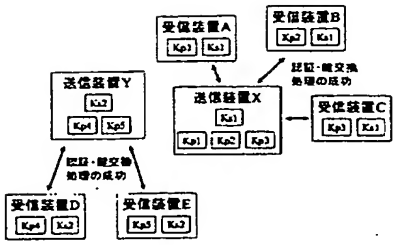
【図１】



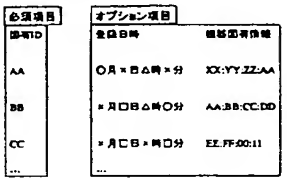
【図２】



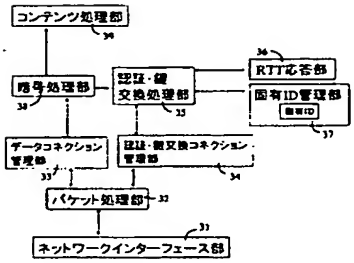
【図３】



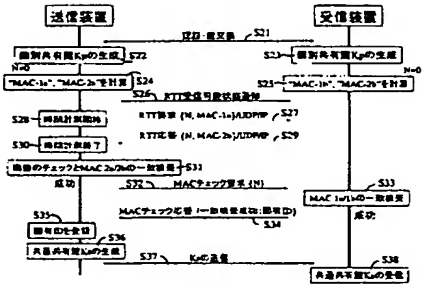
【図４】



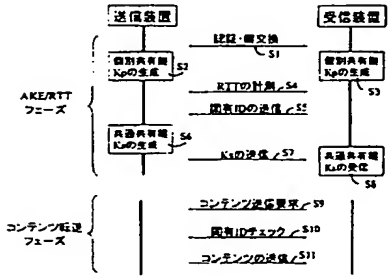
【図５】



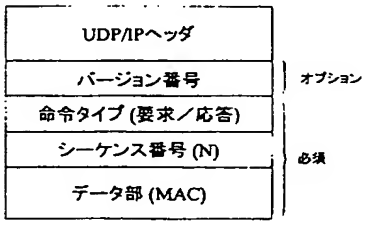
【図７】



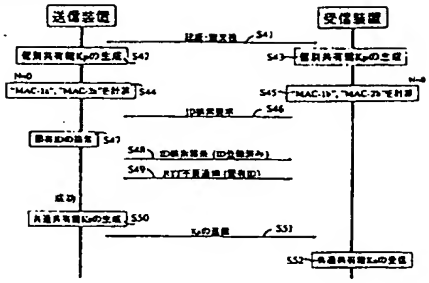
【図６】



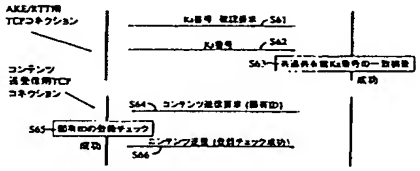
【図８】



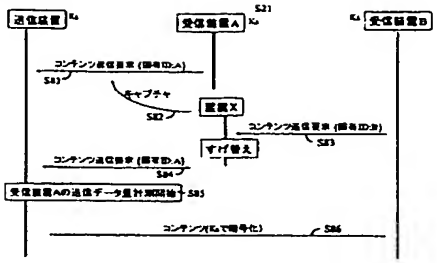
【図９】



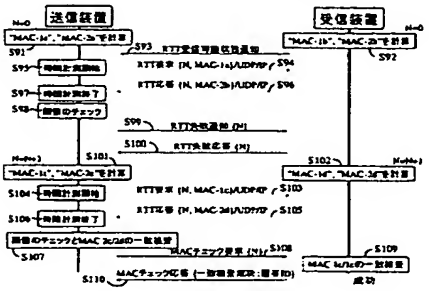
【図１０】



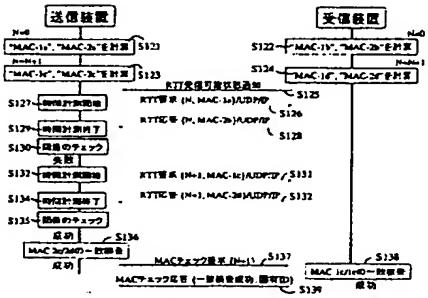
【図１１】



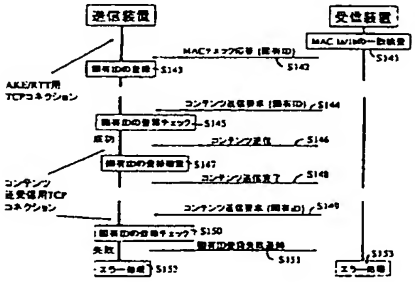
【図１２】



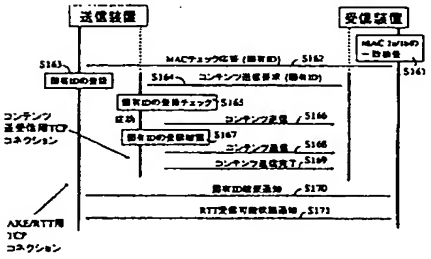
【図１３】



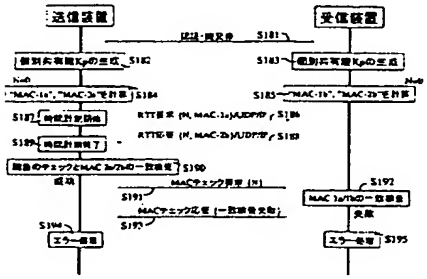
【図１４】



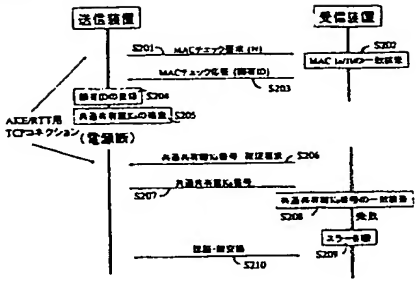
【図１５】



【図１６】



【図１７】


送信装置
受信装置
S201
S202
S203
S204
S205
AES/RTT用
TCPコネクション（確立後）
S206
S207
S208
S209
S210

フロントページの続き

(72)発明者 磯 崎 宏
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 小久保 隆
東京都青梅市末広町２丁目９番地 株式会社東芝青梅事業所内
(72)発明者 金 澤 浩 二
東京都青梅市末広町２丁目９番地 株式会社東芝青梅事業所内

Ｆターム(参考) 5J104 AA07 AA16 EA17 EA18 KA04 PA07
5K035 AA06 BB01 DD01 GG06 HH02